UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/728,396	12/05/2003	Anthony J. Yeates	M61.12-0576	9252

27366 7590 09/28/2007

WESTMAN CHAMPLIN (MICROSOFT CORPORATION)
SUITE 1400
900 SECOND AVENUE SOUTH
MINNEAPOLIS, MN 55402-3319

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
09/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/728,396	YEATES ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-23* is/are pending in the application.

4a) Of the above claim(s) *2* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 AND 3-23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-23 are pending.

Response to Arguments

2. *Applicant's arguments with respect to claims 1-13 and 21-23 have been considered but are moot in view of the new ground(s) of rejection.*

Independent claim 1 is currently amended to include the limitations of dependent claim 2 that is now cancelled.

In addition, claims 1 and 21 introduces new limitation of the encryption component being a collection of data that specifies an encryption or decryption process. For this reason, new grounds of rejection is applied and the rejection is final. Sutter discloses tables containing records or collections of data that specifies user-specific information (i.e. password, private key) and permissions according to users (col.14, lines 5-23 and col.48, line 60 – col.49, line 65 and col.51, lines 21-67). Sutter obviously suggests the encryption component and a collection of data but did not clearly explain the encryption component being a collection of data that specifies an encryption or decryption process. Thus, Sutter is combined with Nguyen to teach that would have been obvious for a person of ordinary skills in the art the encryption component being a collection of data that specifies an encryption or decryption process (Nguyen - col.5, lines 14-41) because the improved encryption approach is efficient and minimize overhead costs that provides good protection again common types of attacks and

reduces the load on a processor (Nguyen - col.2, lines 2, lines 35-40 and col.3, lines 12-22 and col.5, lines 52-58). Claims 1 and 21 are materially amended introducing new limitation. For this reason, the amendment is necessitated by new grounds of rejection and the rejection is made final.

According to the argument on pg.2 (2nd paragraph), that the process for logging in and authenticating the use in no way involves utilizing a received password as a basis for generation of user-specific version of an encryption component as claimed. Sutter discloses the user (e.g. site operator or administrator) password is specific to an encryption key because the user selects the password from which derives a key that is used for encryption (col.51, lines 47-65 and col.89, lines 30-46). Sutter gives many examples of the key value, encrypted with a key derived from the site's administrator password (col.34, lines 30-34 and col.49, lines 20-29). Thus, the key derived from the password given at logon read on the claimed utilizing a received password as a basis for generation of user-specific version of an encryption component.

Examiner traverses the argument on pg.2 (3rd paragraph), failing to teach selectively allowing the user process to process to the user-specific version of the encryption component so as to derive the encryption component. Only claim 1 is being traversed and responded to because independent claim 21 does not recite this limitation. Sutter discloses tables containing records or collections of data that specifies user-specific information (i.e. password, private key) and permissions according of users (col.14, lines 5-23 and col.48, line 5 – col.49, line 65 and col.51, lines 21-67). Permissions are also known as rules or privileges to grant access to/for a particular

person, device, system, etc. to secure data or files (col.73, lines 50-56). Hence, Sutter suggests selectively allowing a user because it is obvious certain permission(s) is for particular user(s) and not all users. For instance, the permission allows a user to a particular encryption component or the permission allows a selected user to process a selection of encryption components (col.73, lines 50-56 and col.74, lines 60-67). In Sutter's invention, the permission applies to a particular user to gain access at various sites and services that users and sites can selectively use and the database includes tables used to store security (sensitive) and other application-specific information (col.6, lines 45-48 and col.40, lines 50-58). Sutter's permission, password, encryption key, and security information are all specific to a particular user (col.14, lines 5-15 and col.48, line 5 – col.49, line 65), suggests the claimed selectively allowing the user to process the user-specific version of the encryption component so as to derive the encryption component.

3. *Applicant's arguments filed 7/10/07, for claims 14-20 have been fully considered but they are not persuasive.*

Claims 14-20 was not amended and therefore remains rejected in view of the Sutter reference. Applicant's argument on pg.2 (2nd paragraph) does not apply for independent claim 14 because it fails to limit receiving a password from a user and utilizing a received password as a basis for generation of user-specific version of an encryption component. As for the argument regarding the 3rd paragraph, please refer above.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 14-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Sutter (US 6,446,092).

Claim 14

Sutter discloses a computer-readable medium having instructions embedded thereon that, when executed, cause a computer to carry out a method comprising the steps of:

obtaining an encryption component; and **(col.14, lines 57-60 and col.45, lines 49-52)**

creating and storing a plurality of user-specific versions of the encryption component; **(col.13, lines 18-20 and col.45, lines 45-52)**

selectively allowing users to process **(col.87, lines 39-45)** their version of the encryption component so as to derive the encryption component; and **(col.15, lines 50-55 and col.51, lines 21-67)**

utilizing the encryption component to process sensitive data. **(col.73, lines 50-56 and col.74, lines 60-67)**

Sutter discloses tables containing records or collections of data that specifies user-specific information (i.e. password, private key) and permissions according of

users (col.14, lines 5-23 and col.48, line 60 – col.49, line 65 and col.51, lines 21-67). Sutter discusses tables with collections of data (col.36, lines 25-37) such as permissions, private keys specific to the user that is encryption process related, and selectively allowing a user (col.73, lines 50-56 and col.74, lines 60-67). In Sutter's invention, the permission applies to a particular user to gain access at various sites and services that users and sites can selectively use and the database includes tables used to store security (sensitive) and other application-specific information (col.6, lines 45-4 and col.40, lines 50-58). Sutter's permission, password, encryption key, and security information are all specific to a particular user (col.14, lines 5-15 and col.48, line 5 – col.49, line 65). Thus, reads on selectively allowing the user to process the user-specific version of the encryption component and utilizing the encryption component to process sensitive data (col.51, lines 21-67 and col.74, lines 60-67).

Claim 15: See Sutter on col.51, lines 20-25 and 55-58 and col.88, lines 58-59; discussing a method of claim 14, wherein storing a plurality of user-specific versions comprises storing a user-specific version in a user account for each of a plurality of users.

Claim 16: See Sutter on col.89, lines 53-55; discussing a method of claim 14, wherein obtaining an encryption component comprises obtaining an application security encryption key.

Claim 17: See Sutter on col.89, lines 43-46 and 53-57; discussing a method of claim 14, wherein creating a plurality of user-specific versions comprises encrypting the encryption component based on a plurality of different user passwords.

Claim 18: See Sutter on col.6, lines 45-48 and col.40, lines 50-58; discussing a method of claim 14, wherein selectively allowing users to process their version of the encryption component comprises authenticating users and only allowing authorized users to process their version of the encryption component.

Claim 19: See Sutter on col.51, lines 54-65 and col.89, lines 30-46; discussing a method of claim 18, wherein authenticating users comprises, for each user: receiving a password; processing the password to generate an encrypted version; and comparing the encrypted version to an authorized value.

Claim 20: See Sutter on col.36, lines 5-10; discussing a method of claim 19, wherein processing the password comprising applying a one-way hash algorithm.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-13 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sutter (US 6,446,092), and further in view of Nguyen, et al. (US 7,194,621).

Claim 1:

Sutter discloses a computer-implemented method for providing data security, the method comprising:

receiving a password from a user; **(col.14, lines 47-48 and col.51, lines 47-51;** *Sutter refers to the claimed password as a password or a pass-phrase received or entered at logon.***)**

utilizing the password as a basis for generation of a user-specific version of an encryption component **(col.51, lines 54-65 and col.89, lines 30-46),** *[the encryption component being a collection of data that specifies an encryption or decryption process]*; **(col.36, lines 25-37)**

storing the user-specific version of the encryption component; and **(col.13, lines 18-20 and col.45, lines 45-52)**

selectively allowing the user to process the user-specific version **(col.87, lines 39-45)** of the encryption component so as to derive the encryption component; and **(col.15, lines 50-55 and col.51, lines 21-67)**

utilizing the encryption component to process sensitive data. **(col.73, lines 50-56 and col.74, lines 60-67)**

Sutter discloses the user (e.g. site operator or administrator) password is specific to an encryption key of the application because the user selects the password from which derives a key that is used for encryption (col.51, lines 47-65 and col.89, lines 30-46). Sutter gives many examples of the key value, encrypted with a key derived from the site's administrator password (col.34, lines 30-34 and col.49, lines 20-29). Thus,

Sutter reads on the claimed invention. Further, Sutter discloses tables containing records or collections of data that specifies user-specific information (i.e. password, private key) and permissions according of users (col.14, lines 5-23 and col.48, line 60 – col.49, line 65 and col.51, lines 21-67). Thus, suggests selectively allowing the user to process the user-specific version of the encryption component and utilizing the encryption component to process sensitive data (col.51, lines 21-67 and col.74, lines 60-67). Sutter discusses tables with collections of data (col.36, lines 25-37) such as permissions, private keys specific to the user that is encryption process related, and selectively allowing a user (col.73, lines 50-56 and col.74, lines 60-67). However, Sutter did not clearly explain the encryption component being a collection of data that specifies an encryption or decryption process.

Nguyen, discloses the client includes a data storage device and a client process stores data in one or more data structures in storage that is accessible to the client process (col.5, lines 14-18). Further, client hosts a selective encryption and decryption process or encryption service which selectively callable by client process to carry out encryption and decryption functions (col.5, lines 31-41). The encryption method is selected to provide good protection against common types of attacks and selected to avoid the intensive computations employed by ciphers (col.5, lines 52-58).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine to teach selectively allowing the user to process the user-specific version of the encryption component of Sutter with Nguyen to teach the encryption component being a collection of data that specifies an encryption or decryption process (Nguyen -

col.5, lines 14-41) because the improved encryption approach is efficient and minimize overhead costs that provides good protection again common types of attacks and reduces the load on a processor (Nguyen - col.2, lines 2, lines 35-40 and col.3, lines 12-22 and col.5, lines 52-58).

Claim 2: Cancelled

Claim 3: See Sutter on col.51, lines 20-65 and col.89, lines 30-60 and Nguyen on col.5, lines 52-58; discussing a method of claim 1, wherein storing comprises storing the user-specific version of the encryption component within a record that is associated with the user.

Claim 4: See Sutter on col.51, lines 54-65 and col.89, lines 30-46; discussing a method of claim 1, further comprising: generating an encrypted version of the password; and storing the encrypted version of the password.

Claim 5: See Sutter on col.51, lines 54-65 and col.89, lines 30-46; discussing a method of claim 4, wherein storing the encrypted version of the password comprises storing the encrypted version of the password within a record that is associated with the user.

Claim 6: See Sutter on col.36, lines 5-10; discussing a method of claim 4, wherein generating an encrypted version of the password comprises encrypting the password based on a one-way hash function.

Claim 7: See Sutter on col.48, lines 10-18 and col.51, lines 54-58; discussing a method of claim 1, further comprising: receiving a second password from a different user; and utilizing the second password as a basis for generation of a second user-

specific version of the encryption component; and storing the second user-specific version of the encryption component.

Claim 8: See Sutter on col.36, lines 25-38 and col.48, lines 10-18; discussing a method of claim 7, wherein storing comprises storing the second user-specific version of the encryption key within a record that is associated with the different user.

Claim 9: See Sutter on col.51, lines 54-58 and col.89, lines 30-46; discussing a method of claim 7, further comprising: generating an encrypted version of the second password; and storing the encrypted version of the second password within a record that is associated with the second user.

Claim 10: See Sutter on col.36, lines 25-37 and col.52, lines 7-12; discussing a method of claim 1, further comprising: receiving an administrator password from an administrator; and utilizing the administrator password as a basis for generation of an administrator-specific version of the encryption component; and storing the administrator-specific version of the encryption component.

Claim 11: See Sutter on col.34, lines 32-34 and Nguyen on col.5, lines 52-58; discussing a method of claim 10, wherein storing comprises storing the administrator-specific version of the encryption key within a record that is associated with the administrator.

Claim 12: See Sutter on col.35, lines 63-65 and col.45, lines 50-52; discussing a method of claim 10, further comprising: generating an encrypted version of the administrator password; and storing the encrypted version of the administrator password within a record that is associated with the administrator.

Claim 13: See Sutter on col.36, lines 25-37 and col.52, lines 7-12; discussing a method of claim 1, wherein utilizing the password as a basis for generation of a user-specific version of an encryption component comprises utilizing the password as a basis for generation of a user-specific version of an application security key.

Claim 21:

Sutter discloses a computer implemented method of providing data security, the method comprising:

receiving a password from a user; **(col.14, lines 47-48 and col.51, lines 47-51;** *Sutter refers to the claimed password as a password or a pass-phrase received or entered at logon.***)**

processing the password to form an encrypted version; **(col.51, lines 54-65 and col.89, lines 30-46)**

comparing the encrypted version to a list of authorized values stored in a database; **(col.51, lines 21-67 and col.74, lines 60-67)**

if the encrypted version matches an authorized value **(col.89, lines 8-15)**, and if doing so would be consistent with a plurality of allocated user access privileges **(col.14, lines 5-23 and col.88, lines 58-59)**, utilizing the password as a basis for decrypting a user-specific version of an encryption component, *[the encryption component being a collection of data that specifies an encryption or decryption process]*; and **(col.36, lines 25-37 and col.52, lines 7-12)**

utilizing the encryption component to process sensitive data. **(col.73, lines 50-56 and col.74, lines 60-67)**

Sutter discloses tables containing records or collections of data that specifies user-specific information (i.e. password, private key) and permissions according of users (col.14, lines 5-23 and col.48, line 60 – col.49, line 65 and col.51, lines 21-67). Thus, suggests selectively allowing the user to process the user-specific version of the encryption component and utilizing the encryption component to process sensitive data (col.51, lines 21-67 and col.74, lines 60-67). Sutter discusses tables with collections of data (col.36, lines 25-37) such as permissions, private keys specific to the user that is encryption process related, and selectively allowing a user (col.73, lines 50-56 and col.74, lines 60-67). However, Sutter did not clearly explain the encryption component being a collection of data that specifies an encryption or decryption process.

Nguyen, discloses the client includes a data storage device and a client process stores data in one or more data structures in storage that is accessible to the client process (col.5, lines 14-18). Further, client hosts a selective encryption and decryption process or encryption service which selectively callable by client process to carry out encryption and decryption functions (col.5, lines 31-41). The encryption method is selected to provide good protection against common types of attacks and selected to avoid the intensive computations employed by ciphers (col.5, lines 52-58).

Therefore, it would have been obvious for a person of ordinary skills in the art to combine to teach selectively allowing the user to process the user-specific version of the encryption component of Sutter with Nguyen to teach the encryption component being a collection of data that specifies an encryption or decryption process (Nguyen - col.5, lines 14-41) because the improved encryption approach is efficient and minimize

overhead costs that provides good protection again common types of attacks and reduces the load on a processor (Nguyen - col.2, lines 2, lines 35-40 and col.3, lines 12-22 and col.5, lines 52-58).

Claim 22: See Sutter on col.54, lines 57-60 and col.85, lines 25-36 and Nguyen on col.5, lines 52-58; discussing a method of claim 21, wherein the plurality of allocated user access privileges are distributed based on a plurality of user roles, and wherein the method further comprises making the step of utilizing the encryption component contingent upon the user being associated with a particular user role.

Claim 23: See Sutter on col.51, lines 20-65 and col.54, lines 57-60; discussing a method of claim 21, wherein the plurality of allocated user access privileges are distributed based on user identity, and wherein the method further comprises making the steps of utilizing the encryption component contingent upon the user having a particular identity.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100